

What Is Claimed Is:

1 1. A method for managing user attributes in a distributed computing
2 system, wherein user attributes determine access rights to a computer application:
3 the method comprising:
4 modifying an attribute database, wherein the attribute database includes a
5 plurality of possible user attributes and a plurality of users;
6 obtaining an identity certificate from a certificate authority;
7 associating the identity certificate with a user from the plurality of users
8 within the attribute database;
9 assigning an attribute from the plurality of possible user attributes to the
10 user, whereby the user is granted access rights based on the attribute and the
11 identity certificate;
12 storing the attribute assigned to the user in the attribute database; and
13 distributing modifications to the attribute database to a plurality of hosts
14 coupled together by a network.

1 2. The method of claim 1, further comprising:
2 assigning a second attribute from the plurality of possible user attributes to
3 the user; and
4 storing the second attribute assigned to the user in the attribute database.

1 3. The method of claim 1, further comprising using secure
2 communications for distributing modifications to the attribute database to the
3 plurality of hosts.

9 associating the identity certificate with a user from the plurality of users
10 within the attribute database;

11 assigning an attribute from the plurality of possible user attributes to the
12 user, whereby the user is granted access rights based on the attribute and the
13 identity certificate;

14 storing the attribute assigned to the user in the attribute database; and

15 distributing modifications to the attribute database to a plurality of hosts
16 coupled together by a network.

1 10. The computer-readable storage medium of claim 9, the method
2 further comprising:

3 assigning a second attribute from the plurality of possible user attributes to
4 the user; and

5 storing the second attribute assigned to the user in the attribute database.

1 11. The computer-readable storage medium of claim 9, the method
2 further comprising using secure communications for distributing modifications to
3 the attribute database to the plurality of hosts.

1 12. The computer-readable storage medium of claim 9, the method
2 further comprising signing the attribute database with a cryptographic signature to
3 allow detection of unauthorized changes to the attribute database.

1 13. The computer-readable storage medium of claim 9, wherein a host
2 of the plurality of hosts can distribute modifications to the attribute database to a
3 subordinate host in a tree architecture.

1 14. The computer-readable storage medium of claim 9, the method
2 further comprising allowing the user to assume any attribute stored in the attribute
3 database that is assigned to the user.

1 15. The computer-readable storage medium of claim 9, the method
2 further comprising:
3 deleting the attribute assigned to the user from the attribute database; and
4 redistributing the attribute database to the plurality of hosts.

1 16. The computer-readable storage medium of claim 9, wherein
2 modifying the attribute database includes creating the attribute database.

1 17. An apparatus that facilitates managing user attributes in a
2 distributed computing system, wherein user attributes determine access rights to a
3 computer application: the apparatus comprising:
4 a modifying mechanism configured to modify an attribute database,
5 wherein the attribute database includes a plurality of possible user attributes and a
6 plurality of users;
7 an identity certificate obtaining mechanism configured to obtain an
8 identity certificate from a certificate authority;
9 an associating mechanism configured to associated the identity certificate
10 with a user from the plurality of users within the attribute database;
11 an assigning mechanism configured to assign an attribute from the
12 plurality of possible user attributes to the user, whereby the user is granted access
13 rights based on the attribute and the identity certificate;
14 a storing mechanism configured to store the attribute assigned to the user
15 in the attribute database; and

16 a distributing mechanism that is configured to distribute modifications to
17 the attribute database to a plurality of hosts coupled together by a network.

1 18. The apparatus of claim 17, further comprising:
2 the assigning mechanism that is further configured to assign a second
3 attribute from the plurality of possible user attributes to the user; and
4 the storing mechanism that is further configured to store the second
5 attribute assigned to the user in the attribute database.

1 19. The apparatus of claim 17, further comprising a secure
2 communications mechanism configured to distribute modifications to the attribute
3 database to the plurality of hosts.

1 20. The apparatus of claim 17, further comprising a signing
2 mechanism that is configured to sign the attribute database with a cryptographic
3 signature to allow detection of unauthorized changes to the attribute database.

1 21. The apparatus of claim 17, wherein the communications
2 mechanism associated with a host of the plurality of hosts is configured to
3 distribute modifications to the attribute database to a subordinate host in a tree
4 architecture.

1 22. The apparatus of claim 17, further comprising an authorization
2 mechanism that is configured to authorize the user to assume any attribute stored
3 in the attribute database that is assigned to the user.

1 23. The apparatus of claim 17, further comprising:

2 a deleting mechanism that is configured to delete the attribute assigned to
3 the user from the attribute database; and
4 a redistributing mechanism that is configured to redistribute the attribute
5 database to the plurality of hosts.

1 24. The apparatus of claim 17, wherein the modifying mechanism is
2 further configured to create the attribute database.